Be aware, don’t fund terrorism

By Kimball Johnson

NCO Journal

Feb. 28, 2018

Terrorism needs money to meet its goals. NCOs can help their Soldiers learn how to avoid becoming unintentional contributors to a terrorist bank account and how to detect possible illegal activities operated by terrorists by understanding how these organizations raise money. (U.S. Army photo by Sgt. Sinthia Rosario, Task Force Lifeliner Public Affairs)

Like any organized endeavor, terrorism needs money to meet its goals. Explosives and electronics are expensive, while logistically, terrorists require training, travel funds, food, and safe houses for staging.

Although Army Regulation 525-13, Antiterrorism stipulates terrorist awareness training for Soldiers, it does not address how terrorists raise money. NCOs can help their Soldiers learn how to avoid becoming unintentional contributors to a terrorist bank account and how to detect possible illegal activities operated by terrorists by understanding how these organizations raise money.

Intellectual Piracy

Until recently, IP has been a primary source of income for many terrorist organizations. It includes the illegal copying and selling of DVDs, CDs, software, and electronic games.

"Terrorist groups, especially those in developing nations, thrive on piracy allowing for the successful funding of terrorist opportunities. Terrorist groups gravitate towards IP for funding because detection of piracy is easily evaded and developing nations do not thoroughly understand it," said Brandy Robinson, Michigan state attorney and author of an in-depth study of the problem.[1]

NCOs assigned to overseas locations are familiar with how available pirated media is. However, NCOs and Soldiers alike may not be aware of how terrorist organizations get their funding from such purchases.

Some examples (http://copyright.nova.edu/piracy-funds-terrorism-google-removes-youtube-videos/) for NCOs to refer to, for instructional purposes, of how funds, raised through the sale of bootleg items, have helped to fund terrorism are as follows:

- International authorities found that Al Qaeda training materials suggested using counterfeit goods and materials to fund its cell activities.
- British detectives claim that Pakistani DVDs account for 40 percent of anti-piracy confiscations in the United Kingdom and that profits from pirated DVDs funnel back to the coffers of Pakistan-based Al Qaeda operatives.
- In 1994, the terrorist group, Hezbollah, used the illicit counterfeiting industry to fund its bombing of the Jewish Community Center in Buenos Aires.
- In the aftermath of the 2008 London bombings, authorities identified Mohammad Sidique Khan, a bootleg CDs and DVDs dealer in South Africa, as one of the coordinators of the bombings.
- Argentina, Brazil, and Paraguay (a tri-border area) serve as a regional hub for terrorist organizational funding for groups such as Hezbollah and Hamas. This fundraising includes counterfeit American goods, including Microsoft software. Hezbollah receives upwards of twenty million dollars annually from illegal IP activities.
- There was a $2.5 million transfer from DVD pirate Assad Ahmad Barakat to Hezbollah, who received a "thank you" note from its leader.[2]

eBay for Terrorists

Intellectual piracy of media isn't the only way that terrorists raise funds. Online sales of items by international, as well as national sellers, who never plan to provide the merchandise, can also be a source.

In August 2017, an article by news reporter Doreen McCallister stated that the FBI had tracked a global financial network that used fake eBay transactions to funnel money to their operatives in the U.S.[3]

One of their self-confessed operatives, Mohamed El Shinawy, of Edgewood, Maryland, pled guilty "to conspiring to provide material support to the Islamic State of Iraq and al-Sham:"[4]

> "The government had alleged in a 2016 indictment that the American operative, Mohamed El

> "The government had alleged in a 2016 indictment that the American suspect, Mohamed El Shinawy, pledged allegiance to Islamic State and had pretended to sell computer printers on eBay as a cover to receive payments through PayPal, potentially to fund terror attacks ... he was instructed to use the money for 'operational purposes' in the U.S., such as a possible terror attack."[5]

According to the Justice Department and a separate article by news reporters Mark Maremont and Christopher S. Stewart of The Wall Street Journal,[6] El Shinawy received $8,700 via PayPal payments to plan and fund a terrorist attack.

This relatively small amount of money, received via a popular payment service, highlights the recent change in terrorist tactics where terrorists avoid large, well-planned operations to focus their support on random acts of individual terrorism that are cheaper to fund and less likely to be discovered.

NCOs can warn their Soldiers, during annual terrorism briefings, to be wary of purchasing items from online sources. By researching the sales history of the seller and reviewing comments by previous purchasers, they can avoid sending funds to questionable individuals.

NCOs can also make their Soldiers aware of how to report such fraudulent activities online to the Internet Crime Complaint Center (https://www.ic3.gov/), managed by the FBI.

Cryptocurrency

NCOs and their Soldiers should also be aware of the latest way in which terrorist organizations are trying to raise money through a new form of online payment known as cryptocurrency.[7]

Cryptocurrency is designed to hide the personal information of the persons involved in an online financial transaction.[7] Currently, Bitcoin is the most popular cryptocurrency in circulation and according to a report by the Council on Foreign Relations (https://www.cfr.org/), a think-thank organization of public officials, businessmen and analysts established in 1921, "Bitcoin and other cryptocurrencies—virtual money—are gaining traction as a source of funding for terrorist groups, such as the self-proclaimed Islamic State."[8]

Terrorists have attempted to fund their activities with greater anonymity by purchasing Bitcoin through stolen identities, credit cards, and banking information, as an incident from December 2017 shows.

> According to Justice Department court filings, the defendant used more than a dozen credit cards — six of which allegedly were fraudulently obtained — to buy approximately $62,700 in Bitcoin and other cryptocurrencies. The government says Zoobia Shahnaz converted the cryptocurrencies back to U.S. dollars and deposited the funds into a checking account in her name. She also allegedly obtained a $22,500 loan from a Manhattan bank. The Justice Department says Shahnaz then began transferring money abroad to support ISIS, while

> Department says Shahnaz then began transferring money abroad to support ISIS, while taking measures to disguise the nature and purpose of the funds and avoid transaction reporting requirements.[9]

Cash Not Accepted Here & the Restaurant Ruse

To add to the potential for further fraudulence, more and more retailers no longer accept cash, making daily electronic purchase transactions a possible source of stolen credit and bankcard information for terrorists.[10]

An article on the website Bankrate (https://www.bankrate.com/finance/credit-cards/5-ways-thieves-steal-credit-card-data-1.aspx) explains how it can happen:

> A waitress whisks away your credit card and swipes it through the restaurant's credit card terminal, which is out of sight. She then pulls out a skimmer (https://www.bankrate.com/credit-cards/what-is-a-skimmer/), a device about the size of an ice cube, and swipes your card through it.
>
> While you were scraping the last of the chocolate frosting off your plate, your credit card information was being stolen. The waitress returns your card with a smile. She performs that same magic trick on dozens of credit cards in a week.
>
> When credit card data ends up in criminal hands, it gets sold. The skimming waitress sells your credit card data for as little as $10 to $20.
>
> The person who buys the information verifies it and then sells it to someone who creates fraudulent credit cards with your account information attached to it.[11]

Our reliance upon credit card convenience has become a target for terrorist and criminal groups and NCOs should consider making credit card theft and its prevention a topic of discussion when preparing their Soldiers for deployments.

Conclusion

Though the fact of how terrorism works to exploit spending habits is worrying, informed NCOs can help their Soldiers learn how to prevent terrorists from using their personal information and funds.

Perhaps the simplest preventative measure for discussion is the disposal of mail and other personal paperwork by shredding or burning instead of just throwing it in the trash. Mail, such as unrequested offers for credit cards, mortgages, and other financing options needs to be properly disposed of so that thieves are unable to steal personal information from the trash.[12]

It also includes warning Soldiers to check card readers at automated teller machines or gas pumps for skimmer devices that slip over the card slot; look before you swipe. Credit card skimmers are becoming so cheap and prevalent that there are now applications for your phone, such as Skimmer Scanner (https://play.google.com/store/apps/details?

id=skimmerscammer.skimmerscammer) that show the locations of where skimmers have been found in your local area and that can alert you when a skimmer signal (https://learn.sparkfun.com/tutorials/gas-pump-skimmers) is detected at the terminal you are currently using.[13]

When making online purchases, Soldiers can carefully review a seller's rating history and investigate how long the business has been selling online, to avoid fraudulent vendors. Soldiers can also avoid trouble online by remembering that purchasing bootleg items is illegal. NCOs can set an example of passing up such "good deals."

However, as regular security briefings make clear, being aware is the most important thing a Soldier can do to prevent becoming a target for identity theft, fraudulence, and terrorism.

Notes

1. Brandy Robinson, "IP Piracy & Developing Nations: A Recipe for Terrorism Funding," *Rutgers Law Record*, Vol. 42, (2014-2015), 42.
2. Stephen Carlisle, "How Copyright Piracy Funds Terrorism and Google Removes 180 Million Videos from YouTube," *NovaSoutheasternUniversity.edu*, March 15, 2015, accessed on January 2, 2018, http://copyright.nova.edu/piracy-funds-terrorism-google-removes-youtube-videos/ (http://copyright.nova.edu/piracy-funds-terrorism-google-removes-youtube-videos/); Brandy Robinson, "IP Piracy," 42-80.
3. Doreen McCallister, "ISIS Used eBay as Part of Terror Network, Unsealed FBI Affidavit Shows,"*npr.com*, August 11, 2017, https://www.npr.org/sections/thetwo-way/2017/08/11/542748232/isis-used-ebay-as-part-of-terror-network-unsealed-fbi-affidavit-shows (https://www.npr.org/sections/thetwo-way/2017/08/11/542748232/isis-used-ebay-as-part-of-terror-network-unsealed-fbi-affidavit-shows).
4. "Maryland Man Pleads Guilty for Conspiring to Provide and for Providing Material Support to ISIS," *Justice.gov*, August 15, 2017, accessed on January 2, 2018, https://www.justice.gov/opa/pr/maryland-man-pleads-guilty-conspiring-provide-and-providing-material-support-isis (https://www.justice.gov/opa/pr/maryland-man-pleads-guilty-conspiring-provide-and-providing-material-support-isis).
5. Mark Maremont and Christopher S. Stewart, "FBI Says ISIS Used eBay to Send Terror Cash to U.S.," *WSJ.com*, August 10, 2017.
6. "Maryland Man Pleads Guilty" & Mark Maremont and Christopher S. Stewart, "FBI Says ISIS Used eBay."
7. David Manheim, Patrick Johnston, Josh Baron & Cynthia Dion-Schwarz, "Are Terrorists Using Cyptocurrencies?" *Foreign Affairs*, (April 2017).
8. Micah Zenko, "Bitcoin for Bombs," *cfr.org*, August 17, 2017, accessed on January 2, 2018, https://www.cfr.org/blog/bitcoin-bombs (https://www.cfr.org/blog/bitcoin-bombs).
9. Laurel Wamsley, "Long Island Woman Charged with Using Bitcoin to Launder Money to Support ISIS," npr.org, December 15, 2017, accessed on January 2, 2018, https://www.npr.org/sections/thetwo-way/2017/12/15/571099023/long-island-woman-charged-with-using-bitcoin-to-launder-money-to-support-isis (https://www.npr.org/sections/thetwo-way/2017/12/15/571099023/long-island-woman-charged-with-using-bitcoin-to-launder-money-to-support-isis).
10. Jay L. Zagorsky, "If Cash Is King, How Can Stores Refuse to Take Your Dollars," *observer.com*, February 21, 2107, accessed January 3, 2018, http://observer.com/2017/02/if-cash-is-king-how-can-stores-refuse-to-take-your-dollars/ (http://observer.com/2017/02/if-cash-is-king-how-can-stores-refuse-to-take-your-dollars/).
11. Janna Herron, "5 Ways Thieves Steal Credit Card Information," *bankrate.com*, December 15, 2107, accessed January 3, 2018, https://www.bankrate.com/finance/credit-cards/5-ways-thieves-steal-credit-card-data-1.aspx

(https://www.bankrate.com/finance/credit-cards/5-ways-thieves-steal-credit-card-data-1.aspx).

12. Ethan Morgan, "Identity Theft: Don't Let it Happen to You," *DVIDS*, May 7, 2012, https://www.dvidshub.net/news/88301/identity-theft-dont-let-happen-you (https://www.dvidshub.net/news/88301/identity-theft-dont-let-happen-you)
13. Lee Mathews, "This App Can Tell You if a Criminal is Trying to Skim Your Credit Card," *Forbes*, September 20, 2017, https://www.forbes.com/sites/leemathews/2017/09/20/this-app-can-tell-you-if-a-criminal-is-trying-to-skim-your-credit-card/#1dc38f2f3833 (https://www.forbes.com/sites/leemathews/2017/09/20/this-app-can-tell-you-if-a-criminal-is-trying-to-skim-your-credit-card/#1dc38f2f3833).